#6

Substitute Specification

METHOD FOR CRYPTOGRAPHIC CONVERSION OF BINARY DATA BLOCKS

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

The present invention relates to the field of electrical communications and computer technology and, more particularly, to the field of cryptographic methods and devices for ciphering of messages (information).

DESCRIPTION OF THE PRIOR ART

The totality of features of the claimed method uses the following terms:

- secret key is binary information known only to the legitimate owner;

- cryptographic conversion is digital data conversion which allows the influence of source data bit on a plurality of output data bits, for example, for the purpose of protecting information from unauthorised reading, generating digital signature, generating modification detection code; some important types of cryptographic conversions are unilateral conversion, hashing and ciphering;

- information hashing is a certain method of forming a so-called hash-code of a fixed size (typically 128 bits) for messages of any size; hashing methods are widely used

that are based on iterative hash functions using block mechanisms of information cryptographic conversion (see Lai X., Massey J.L. Hash Functions Based on Block Ciphers/ Workshop on the Theory and Applications of Cryptographic Techniques. EUROCRYPT'92, Hungary, May 24-28, 1992, Proceedings, p.53-66);

- ciphering is a information conversion process which depends on the secret key and which transforms a source text into a ciphered text representing a pseudo-random character sequence from which obtaining information without the knowledge of the secret key is practically unfeasible;

- deciphering is a process which is reverse to ciphering procedure; deciphering ensures recovering information according to the cryptogram when the secret key is known;

- cipher is a totality of elementary steps of input data conversion using the secret key; the cipher may be implemented in the form of a computer program or as a separate device;

- binary vector is a certain sequence of off-bits and on-bits, such as 1011010011; a specific structure of the binary vector may be interpreted as a binary number if it is assumed that position of each bit corresponds to a binary bit, i.e. the binary vector may be compared with a numerical value which is univocally determined by the binary vector structure;

- cryptanalysis is a method of calculating the secret key for obtaining unauthorised access to ciphered information or developing a method which provides access to the ciphered information without calculating the secret key;

- unilateral conversion is such a conversion of a L-bit input data block into an L-bit output data block which allows to easily calculate the output data block according to

the input block, while calculation of the input block which would transform into randomly selected output block is an essentially impracticable task;

- unilateral function is a function the value of which is easily calculated according to a given argument, however, calculating the argument according to a given function value is a computationally difficult problem; unilateral functions are implemented as a procedural sequence of unilateral conversion of a certain input block (argument), the output value of which is assumed as the function value;

- cryptographic resistance is a measure of safety of ciphered information protection and represents labour intensity measured in the number of elementary operations to be performed in order to recover information according to a cryptogram when the conversion algorithm is known but without the knowledge of the secret key; in the case of unilateral conversions, by cryptographic resistance is meant complexity of calculating of the input block value according to its output value;

- cyclic shift operations depending on converted subblocks or depending on a binary vector are operations of cyclic shift on a number of bits set by the subblock value or by the binary vector value; operations of cyclic shit to the left (right) are designated with the sign "<<<"(">>>"), for example, the notation $B_1<<<B_2$ signifies an operation of cyclic shift to the left of subblock B_1 on the number of bits equal to the value of binary vector B_2; similar operations are basic for the RC5 cipher;

- single-site operation is an operation performed on one operand (data block or binary vector); the subblock value after performing a certain given single-site operation depends only on initial value; an example of the single-site operations are operations of addition, subtraction, multiplication, etc.

Methods are known of block ciphering of data, see, e.g., US standard DES (National Bureau of Standards. Data Encryption Standard. Federal Information Processing Standards Publication 46, January 1977). This method of data block ciphering comprises generating a secret key, splitting the data block being converted into two subblocks L and R and alternate changing the latter by carrying out the operation of bit-for-bit modulo 2 summation on the subblock L and a binary vector which is generated as an output value of a certain function F according to the value of subblock R. Thereupon the blocks are interchanged. Function F in this method is implemented by performing the transposition and stuffing operations carried out on subblock R. This method has a high conversion rate when realised in the form of a specialised electronic circuitry.

However, the known closest prior art method uses a secret key of a small size (56 bits) which makes it vulnerable to cryptanalysis based on finding a key to fit it. The latter is associated with high computer power of modern mass-use computers.

The closest by its technical essence to the claimed method for cryptographic conversion of binary data blocks is the method implemented in the cipher RC5 and described in the work (R.Rivest, The RC5 Encryption Algorithm/ Fast Software Encryption, second International Workshop Proceedings (Leuven, Belgium, December 14-16, 1994), Lecture Notes in Computer Science, v.1008, Springer-Verlag, 1995, pp.86-96). The closest prior art method comprises generating a secret key in the form of a totality of subkeys, splitting an input data block into subblocks A and B, and alternate subblock conversion. The subblocks are transformed by performing on them single-site and dual-site operations. As dual-site operations, modulo 2^n addition operations are used, where n=8, 16, 32, 64 and a modulo 2 bit-for-bit summing operation. As the single-site operation, an operation of cyclic shift to the left is used, whereby the number of bits on

which the subblock being converted is shifted depends on the value of another subblock, this determines dependency of the cyclic shift operation at the current step of subblock conversion on the initial value of the input data block. The dual-site operation is performed on a subblock and subkey as well as on two subblocks. Characteristic of the closest prior art method is the use of cyclic bit shift operation of one of subblocks depending on the value of another subblock.

A subblock, for example subblock B, is converted as follows. A modulo 2 bit-for-bit summing operation ("⊕") is performed on subblocks A and B and the value obtained following this operation is assigned to subblock B. This is written as a relation:

$$B \leftarrow B \oplus A,$$

where the sign "←" signifies the assignment operation. After that, the operation of cyclic shift on the number of bits equal to the value of subblock A is performed on subblock B:

$$B \leftarrow B <<< A.$$

Then the modulo 2^n summing operation is performed on the subblock and one of subkeys S: $B \leftarrow (B + S) \bmod 2^n$, where n is the subblock length in bits. After this, subblock A is converted in the similar way. Several such conversion steps are performed for the both subblocks.

This method provides high encryption rate when implemented in the form of a computer program or in the form of electronic ciphering devices. However, the closest prior art has some disadvantages, namely, it fails to ensure high resistance of cryptographic data conversion to differential and linear cryptanalysis (Kaliski B.S., Yin Y.L. On Differential and Linear Cryptanalysis of the RC5 Encryption Algorithm. Advances in Cryptology-CRYPTO'95 Proceedings, Springer-Verlag, 1955, pp.171-184). This disadvantage is due to the fact that effectiveness of the use of operations dependent

on data being converted, with the aim of enhancing ciphering resistance to known cryptanalysis methods, is reduced by the fact that the number of potentially realisable versions of cyclic shift operations is equal to the number of binary bits of subblock n and does not exceed 64.

The basis of the invention is formed by the task to develop a method of cryptographic conversion of binary data blocks, wherein input data conversion would be effected in such a manner as to provide the increase in the number of various versions of an operation which depends on the block being converted due to which resistance to differential and linear cryptanalysis is increased.

SUMMARY OF THE INVENTION

The task is achieved by the fact that in a method of cryptographic conversion of binary data blocks, comprising splitting a data block into $N \geq 2$ subblocks, alternate converting the subblocks by performing on the i-th, where $i \leq N$, subblock at least one conversion operation, said operation depending on the value of the j-th, where $j \leq N$, subblock, while the new feature, according to the invention, is the fact that as the operation dependent on the value of the j-th subblock, a transposition operation of the bits of the i-th subblock is used.

Due to such solution, the number of possible versions of the j-th subblock value dependent operation is increased which enables to enhance cryptographic conversion resistance to differential and linear cryptanalysis.

A novel feature is also that the transposition operation of the bits of the i-th subblock which depends on the value of the j-th subblock is formed depending on a secret key before the beginning of the i-th subblock conversion.

Due to such solution, modification of the transposition operation of the bits of the i-th subblock which depends on the value of the j-th subblock is not predetermined which provides additional enhancement of cryptographic conversion resistance to differential and linear cryptanalyses and allows to reduce the number of conversion operations and thereby to increase ciphering rate.

A novel feature is also that before performing current operation of transposing of the bits of the i-th subblock which depends on the j-th subblock, a binary vector V is additionally generated, while the transposition operation of the bits of the i-th subblock is performed depending on the value of V, whereby the binary vector is generated depending on its value at the time of performing the previous conversion step for one of subblocks and on the value of the j-th subblock.

Due to such solution, additional enhancement of cryptographic resistance is provided to attacks based on break-downs of the ciphering device.

Below the essence of the invention will be clarified in more detail by way of its embodiments with references to attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig.1 presents a generalised diagram of cryptographic conversion according to the claimed method.

Fig.2 schematically presents the structure of controlled transposition block.

Fig.3 represents the structure of controlled transposition block having a 32-bit information input.

Fig.4 presents a block diagram of elementary switch.

Fig.5 presents a table of input and output signals of the elementary switch when u=1 is control signal.

Fig.6 presents a table of input and output signals of the elementary controlled switch when the value of the control signal is u=0.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The invention is explained with a generalised diagram of data block conversion based on the claimed method which is shown in Fig.1,

where: P is the controlled transposition block; A and B are converted n-bit subblock; K_{4r}, K_{4r-1}, K_{4r-2}, K_{4r-3} are n-bit secret key elements (n-bit subkeys); V is binary vector generated depending on input data; $\oplus$ symbol signifies modulo 2 bit-for-bit summing operation; [+] sign denotes modulo n summing operation, where n is the data subblock length in bits. Bold solid lines designate the n-bit signal transmission bus, thin solid lines signify transmission of one bit, thin dotted lines signify transmission of one control bit. Bold dotted lines signify n control signal transmission bus, n control signals being subkeys bits or binary vector bits. Using the subkey bits as control signals ensures forming a specific modification of subblock bit transposition operation dependent on the value of an input block which additionally enhances resistance of cryptographic conversion.

Fig.1 shows one round of conversions. Depending on a specific implementation of controlled transposition block and the required conversion rate, from 2 to 16 and more rounds may be set. This scheme of cryptographic conversion procedures may be used ciphering and for unilateral conversions. In the latter case, the secret key is not used, and instead of subkey signals, the control input of the block P is fed with signals of the binary vector V generated depending on the value of subblocks being converted at intermediate conversion steps. When ciphering, the same four n-bit subkeys K_4, K_3, K_2 and K_1 may be used in carrying out each ciphering round. In this case, when the typical subblock size is n=32, the secret key length is 128 bits. When secret key of a larger size is employed, each round may use K_{4r}, K_{4r-1}, K_{4r-2} and K_{4r-3}. For example, when the round number is r=3, the first round uses subkeys K_4, K_3, K_2, and K_1, the second round uses subkeys K_8, K_7, K_6 and K_5, the third round uses subkeys K_{12}, K_{11}, K_{10} and K_9.

The possibility of technical implementation of the claimed method is explained with its following specific embodiments.

Example 1.

This example relates to the use a method for ciphering data. The secret key is presented in the form of four subkeys K_{4r}, K_{4r-1}, K_{4r-2}, and K_{4r-3}. One ciphering round is described by the following procedural sequence:

1. Convert subblock A according to expression:

$$A \leftarrow A \oplus K_{4r-3},$$

where "$\leftarrow$" is designation of assignment operation.

2. Convert subblock B according to expression:

$$B \leftarrow B\ [+]\ K_{4r-2}.$$

3. Depending on the value of subblock A and on subkey K_{4r-1}, to effect transposition of bit of subblock .

4. Convert subblock A according to expression:

$$A \leftarrow A\ [+]\ B.$$

5. Depending on the value of subblock B and on subkey K_{4r}, effect transposition of bits of subblock A.

6. Convert subblock B according to expression:

$$B \leftarrow B \oplus A,$$

Example 2.

This example describes one round of unilateral conversions according to the following procedural sequence:

1. Generate binary vector V:

$$V \leftarrow A <<< B.$$

2. Convert subblock B according to expression:

$$B \leftarrow B\ [+]\ V.$$

3. Generate binary vector V depending on its value at the previous step and on the values of subblocks A and B according to formula:

$$V \leftarrow (V <<< A) \oplus (B <<< 13).$$

4. Convert subblock A according to expression:

$$A \leftarrow A \oplus V.$$

5. Depending on the values of A and V, effect transposition of bits of subblock B.

6. Convert subblock A according to expression:

$$A \leftarrow A\ [+]\ B.$$

7. Generate binary vector V:

$$V \leftarrow (V <<< B) \oplus (A <<< 11).$$

8. Depending on the values B and V effect transposition of bits of subblock A.

9. Convert subblock B according to expression:

$$B \leftarrow B \oplus A.$$

Fig.2 shows a possible embodiment of the controlled transposition block using the totality of elementary switched S. This embodiment corresponds to the block P having 8-bit input for data signals and 8-bit input for control signals designated with dotted lines similar to designation in Fig.1.

The number of various versions of the transposition operation is equal to the number of possible code combinations at the control input and is $2^8 = 256$ for the block P with the structure presented in Fig.2, which exceeds the number of cyclic shift operations used in the closest prior art method. Using the similar method, it is possible to make up the scheme for block P with an arbitrary size of data input and control signal input, in particular, for block P with 32-bit data input and 32-bit control signal input. In the latter case, the number of different variations of transposition operation equal to $2^{32} > 10^9$ is achieved.

Fig.3 shows the structure of controlled transposition block having 32-bit data input and 79-bit control input. This controlled transposition block implements a unique transposition of input binary bits for each possible value of code combination at the control input the number of which is 2^{79}. External information inputs of the controlled transposition block are designated i1, i2,...., i32, external outputs are designated o1, o2,.....,o32, control inputs are designated c1, c2,...., c79. Elementary switches S are connected in such a way as to form a matrix consisting from 31 lines. In the first line, 31 elementary switches are connected, in the second line, 30, in the third line, 29, etc. In

each subsequent line, the number of elementary switches is reduces by 1. In the lowest line 31, 1 elementary switch is connected.

The number j ≠ 31 line has 33-j inputs, 33-j outputs and 32-j control inputs. The last (rightmost) output of the j-th line is an external output of the controlled transposition block, the remaining 32-j outputs of the j-line are connected to the corresponding inputs of the (j+1)-th line. The last 31 line has two outputs and both of them are external outputs of the controlled transposition block. A unitary (u=1) control signal is supplied to not more than on control input of each line. Binary-32-order decipherers F_1, F_2,....,F_{15} and binary-16-order decipherer F_{16} serve to meet this requirement. Decipherers F_1, F_2,...., F_{15} have five external control inputs to which an arbitrary 5-bit binary code is supplied, and 32 outputs. The decipherers generate a unitary signal only at one output. A zero signal is set at the remaining 31 inputs. Decipherer F_{16} has 4 outputs to which an arbitrary 4-bit binary code is supplied, and 16 outputs only at one of which a unitary signal is set. For all decipherers, F_1, F_2,....., F_{15} and F_{16}, each input binary code value defines a uniquely possible output number at which the unitary signal (u=1) is set.

A part of decipherer F_h outputs, where h ≤15, are connected to control inputs of the h-th line (32-h inputs), while a part of inputs are connected to control inputs of the (32-h)-th line (the remaining h decipherer outputs). The control signal u=1 is set at each line on not more than one elementary switch. The line input connected to the right input of elementary switch to which a unitary control signal is supplied is commuted with the external output of the controlled transposition block corresponding to this line. If the unitary control signal is fed to the leftmost elementary switch, then the external output of the controlled transposition block (block P) is commuted with the leftmost line input. The first line commutes one of the external inputs i1, i2,....., i32 of the block P with the

external output o1, while the remaining 31 external inputs commute with the inputs of the second line. The second line commutes on of the remaining 31 of the external input with the external input o2, while the remaining 30 external inputs commute with the inputs of the 3rd line, and so on. Such structure of the block P implements the unique transposition of input bits for each value of binary code supplied to the 79-bit control input of the block P.

For example, the following version of using the control 79-bit input in the cryptographic conversion scheme, shown in Fig.1, is possible. 32 bits are used as control signals, for example, of subblock B, and 47 bits of the secret key. As the latter, for example, 32 bits of subkey K_{4r-1} and 15 bits of subkey K_{4r-2} may be used. In this case, when the secret key is entered into the ciphering device, depending on these secret key 47 bits, one of 2^{47} different modifications of the bit transposition operation is generated which depends on the input block value. Here each modification of this operation includes 2^{32} of different operations of transposing bits of subblock A selection of which is determined by the value of subblock B. Modification selection is not predetermined since it is determined by the secret key. This additionally enhances resistance of the cryptographic conversion. If the ciphering device employs 4 blocks P having the structure shown in Fig.3, then the number of possible combinations of modifications of the transposition operations being set on clocks P depending on the secret key, may be set up to $(2^{47})^4 = 2^{188}$ using the secret key with a length not less than 188 bits.

Fig.4 clarifies the operation of the elementary switch where u is control signal, a and b are input data signals, c and d are output data signals.

Tables in Fig.5 and 6 demonstrate dependency of output signals on input and control signals. It is apparent from these tables that when u=1, line a is commuted with

line c, and line b with line d. When u=0, line a is commuted with line d, and line b with line d.

Due to the simple structure, the modern planar technology of manufacturing integrated circuits allows to easily produce cryptographic microprocessors comprising controlled transposition blocks with the input size of 32 and 64 bits.

The above examples show that the proposed method for cryptographic conversions of binary data blocks is technically feasible and enables to solve the problem that has been set.

The claimed method may be realised, for example, in specialised cryptographic microprocessors providing ciphering rate in the order of 1 Gbit/s which is sufficient for ciphering in the real time data transmitted over high-speed fibre optic communication channels.